

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-186667

(43)Date of publication of application : 16.07.1996

(51)Int.Cl. H04M 15/00
G06F 15/00
G09C 1/00
G10K 15/04
H04H 1/02
H04L 9/00
H04L 9/10
H04L 9/12
H04N 7/173

(21)Application number : 07-000257

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 05.01.1995

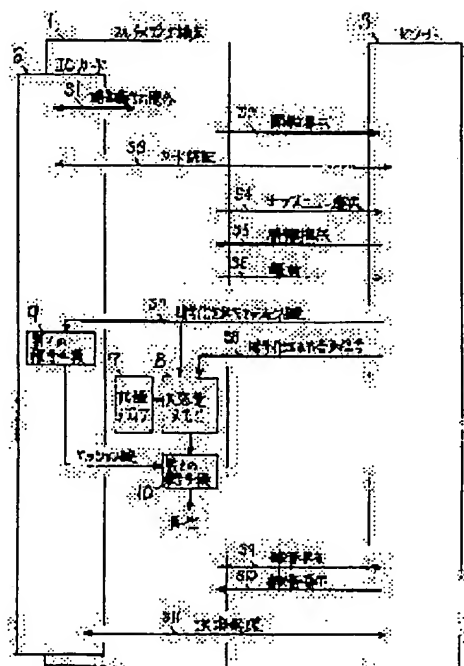
(72)Inventor : TAKAGI SHINYA

(54) DIGITAL INFORMATION RECORDING SYSTEM

(57)Abstract:

PURPOSE: To prevent legal digital copy from being performed by a user while protecting the right of a software author in a system of transmitting music software and video software to individuals through the use of a digital network.

CONSTITUTION: An IC card 6 is used as a control part and has a secret card key (k) peculiar to this card. On the other hand, by a request from a multi-media terminal 1, digital information ciphered by a session key (s) and the session key (s) ciphered by the card key (k) are sent from a center 3 to the multi-media terminal 1 and recorded in a recording media 7. At the time of reproducing digital information, digital information is restored by the session key (s) deciphered in the IC card 6.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-186667

(43) 公開日 平成8年(1996)7月16日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 M 15/00	Z			
G 0 6 F 15/00	3 3 0 Z	9364-5L		
G 0 9 C 1/00		7259-5J		
G 1 0 K 15/04	3 0 2 D			

H 0 4 L 9/00

Z

審査請求 未請求 請求項の数 3 O L (全 9 頁) 最終頁に続く

(21) 出願番号 特願平7-257

(22) 出願日 平成7年(1995)1月5日

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 高木 伸哉

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

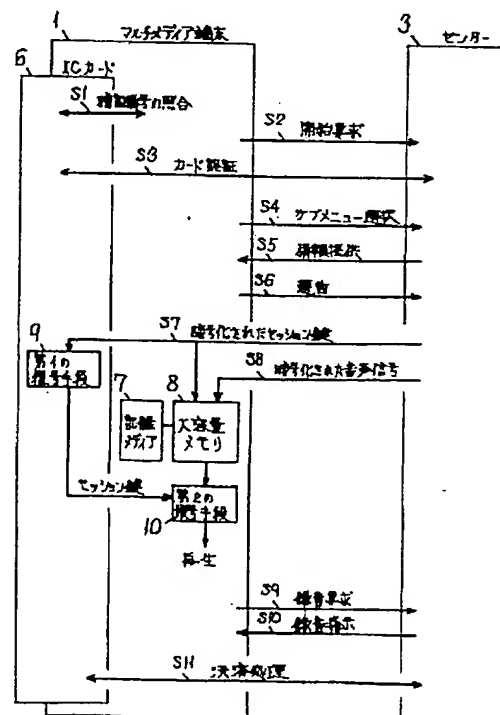
(74) 代理人 弁理士 小鍛冶 明 (外2名)

(54) 【発明の名称】 デジタル情報記録システム

(57) 【要約】

【目的】 デジタルネットワークを用いて音楽ソフトや映像ソフトを個人向けに伝送するシステムにおいて、ソフト著作者の権利を守りながらユーザによる正当なデジタルコピーが防止できるシステムを提供する。

【構成】 ICカード6を制御部として、このカードに固有で秘密のカード鍵kをもたせる一方、マルチメディア端末1からの要求によりセンター3からマルチメディア端末1に、セッション鍵sで暗号化されたデジタル情報と、カード鍵kで暗号化されたセッション鍵sが送られ、記録メディア7に記録される。デジタル情報を再生する際には、ICカード6内で復号されたセッション鍵sによりデジタル情報が復元される。



【特許請求の範囲】

【請求項 1】 デジタル情報のデータベースを保有する情報センターと、この情報センターに接続され前記センターへデジタル情報の送信を要求する要求手段と、デジタル情報を記録メディアへ書き込む書き込み手段とを有する端末を備え前記センターは端末使用者の正否を判断して正の場合に端末からの要求に応じてデジタル情報を端末へ送信する送信手段と、送信したデジタル情報の記録メディアへの書き込み手段を制御する制御手段とを有することを特徴とするデジタル情報記録システム。

【請求項 2】 デジタル情報のデータベースを保有する情報センターと、この情報センターに接続され前記センターへデジタル情報の送信を要求する要求手段と、デジタル情報を記録メディアへ書き込む書き込み手段とを有する端末と第 1 の鍵を格納する格納部を有する IC カードを備え、前記センターは端末使用者の正否を判断して正の場合に端末からの要求に応じてデジタル情報を端末へ送信する送信手段と、送信したデジタル情報の記録メディアへの書き込み手段を制御する制御手段とデジタル情報を暗号化する第 2 の鍵を発生する手段と、前記第 1 の鍵と前記第 2 の鍵から第 3 の鍵を演算する手段と、前記第 2 の鍵によってデジタル情報を暗号化する手段とを有し、前記 IC カードは前記第 1 の鍵と前記センターから送信される第 3 の鍵から第 2 の鍵を演算する手段を有し、端末は前記センターから送信される暗号化されたデジタル情報を前記 IC カードから送信される第 2 の鍵により、デジタル情報を復元する手段を有することを特徴とするデジタル情報記録システム。

【請求項 3】 IC カードは、第 4 の鍵を発生する手段と第 5 の鍵を格納する格納部とを有し、センターの制御手段は、第 4 の鍵と第 1 の鍵から第 5 の鍵を演算し、端末の書き込み手段は、前記第 5 の鍵によって制御されることを特徴とする請求項 2 記載のデジタル情報記録システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、通信回線、例えば大容量のデジタルネットワークを用いて、音楽ソフトや映像ソフトを個人向けに伝送し、記録するシステムに関する。

【0002】

【従来の技術】 近年、通信技術およびコンピュータ技術の発達により、情報のデジタル化が進んでおり、新しい魅力的なサービスが生まれつつある。例えば、これまでの放送とは違い、ユーザが好きな時に見たい映像ソフトを情報センター（以後センターという）要求すると、センターからそのユーザに要求した映像ソフトが送られてくる、いわゆるビデオ・オン・デマンドという新しいシステムが実験的に進められており、注目されている。

【0003】

【発明が解決しようとする課題】 また同様のシステムで映像ソフトではなく、音楽ソフトに関するサービスへも展開が可能である。特に音楽ソフトの場合は映像ソフトと違い 1 曲あたりの時間が短く、繰り返し聴きたい場合も多い。その度にセンターにアクセスするのではユーザにとって料金が嵩んでしまい、またアクセスする手間が面倒であり、更にシステムにおいてトラヒックの問題が発生する。

【0004】 ユーザにとっては、1 回聴くための料金は比較的低額で、気に入った曲は自分の端末にデジタル録音し、それ以降はセンターへアクセスすることなく繰り返し聴けることが望ましい。しかしながら、比較的低額な料金を支払っただけで個人の端末にデジタル録音可能というシステムでは著作権が保護されないという問題がある。

【0005】 また、このシステムにおいてユーザの本人確認が暗証番号の照合で行われているという問題がある。なぜなら暗証番号による、本人確認の安全性の低さは周知の通りであり、サービスが拡大するほど、またサービスが魅力的になるほど不正使用される可能性が大きくなり、本人確認の安全性を高める必要がある。

【0006】 また、このシステムは、システムを利用したユーザではなく、端末に対して課金されるため、ユーザはどの端末でも自由には使用できなかった。その点、ユーザ本人に課金されるシステムであれば、どの端末でも自由にこのシステムを利用できることとなり、利便性が増す。

【0007】 本発明は、上記の問題点を解決するものであり、著作権者の権利を守り、かつ、ユーザによる映像、音楽ソフト等のデジタル記録が可能となるシステムを提供することを目的とするものである。

【0008】 また、ユーザの本人確認の安全性を高め、ユーザ本人に課金されるシステムを提供することを目的とするものである。

【0009】

【課題を解決するための手段】 本発明は上記目的を達成するために、端末に装備される記録メディアへのデジタル情報の書き込み手段は、端末使用者の正否を判断し、正の場合にセンターの制御手段により、制御される構成である。また、端末が IC カードを受け入れる装置を有し、IC カードはそのカードに固有の秘密の鍵コード（以後カード鍵という）を有しており、録音されたデジタル情報は秘密データを用いて演算が施されており、IC カードはカード鍵を用いて前記秘密データを復元する手段を有する構成としたものである。

【0010】

【作用】 上記構成により、デジタル情報はユーザの正否の照合の後、センターの制御によってのみ記録メディアへ記録可能であり、また記録されたデジタル情報は IC カードを用いてのみ再生可能となり、著作権者の権利は保

護される。また、ICカードは秘密のカード鍵を用いることによって、このシステムへのアクセスツールおよび決済ツールとしても使用できるものである。

【0011】

【実施例】

(実施例1) 以下、本発明の一実施例について図面を参照しながら説明する。図1は本発明の一実施例におけるシステムの概略を示す図であり、ユーザが所有するマルチメディア端末1はネットワークISDN2を通して、音楽ソフトを管理しているセンター3および銀行4と接続されている。センター3と銀行4間はこの場合伝送する情報量が多いため、例えば専用回線5で結ばれている。マルチメディア端末1は、ディスプレイ、スピーカの他、ICカード6を挿入するためのリーダライタと、音声信号を録音するための記録メディア7用のドライブを有している。

【0012】図1で示した本システムに用いるICカード6の発行について説明を行う。ユーザがセンター3に対して本システムへの加入申請を行うと、センター3は銀行4にICカード6の発行を依頼する。銀行4はICカード6にユーザの暗証番号や個人情報等、本カードを銀行業務で使用するために必要な情報を書込み、センター3に渡す。センター3ではICカード6に会員番号n、カード鍵kを書き込んでユーザに渡す。ここで、カード鍵kは秘密の暗号鍵であり、次式により算出される。

$$【0013】 k = F(n)$$

ここでFはセンター3のみが知る秘密の関数であり、nは会員番号である。上記式により、カード鍵kは会員番号nの関数であり、それぞれのカードに固有(すなわちユーザに固有)である。ICカード6にこれらを書き込んだ後は、会員番号nを読み出すことは可能であるが、カード鍵kは決して読み出すことができないものである。しかし、センター3はICカード6から会員番号nを読み出すことにより、カード鍵kを再算出することができる。よって、会員番号nとカード鍵kをICカード6に書き込んだ後は、これらの情報をセンター側で持っておく必要はない。

【0014】ユーザはICカード6を受け取った後、マルチメディア端末1(以下、単に端末1と記す)を用いて銀行4にアクセスし、自分の銀行口座の残高の中から希望金額をICカード6内の口座へ移す。もちろん、この処理を行うためには暗証番号の照合が必要であるが、これらの手続きについてここでは詳細は省略する。

【0015】次に、図2を用いて本実施例のシステムを利用する際の処理の流れを説明する。

【0016】まず、ユーザがICカード6を端末1に挿入すると、例えば端末1のディスプレイ上に0~9までの10個の数字と、暗証番号の入力を促すメッセージが出力される。ここでユーザがディスプレイに表示された

数字を指で押し、スイッチの投入で正しい暗証番号を入力することにより、ICカードが暗証番号の照合を行い(ステップS1)、端末1は本システムの利用を開始するための開始要求をセンター3に送信する(ステップS2)。センター3はこの要求を受信することによりサービスを開始する。まず最初にセンター3によるICカード6の認証が行われる(ステップS3)。これはICカード6が正当なカードであるか否かを確認するためのものであり、正当なカードでない場合、サービスは打ち切られる。

【0017】カード認証が正常に終了すると、ディスプレイ上にメインメニューが表示される。このメインメニューは端末1を使用して受けられるサービス等の一覧であり、ユーザはこの中から例えば「音楽鑑賞」を選択する。このメニューが選択されるとディスプレイ上には、ジャンル、アーティスト名、年代等、ユーザが曲を選択する際に手助けとなるサブメニューが表示される。ユーザは例えば聴きたい曲のアーティスト名が決まっている場合は具体的なアーティスト名を指定する。また、タイトルやアーティスト名が不明であったり、聴きたい曲が具体的に決まっていない場合、ディスプレイ上に「冬の情景を描いたフォークソング」といった選択枝を表示し指定させてもよい。このようにユーザがサブメニューから希望の選択枝を指定すると、その情報が端末1からセンター3へ送信される(ステップS4)。センター3は送られてきた情報をもとにデータベースを検索し、該当する全ての曲のタイトルを情報として端末1に提供する(ステップS5)。ユーザがディスプレイに表示されたタイトル一覧から聴きたい曲を指定すると、端末1はセンター3へ選曲情報を送信する(ステップS6)。

【0018】曲が指定されると、センター3は音声信号を暗号化するための鍵をランダムに生成し(以後、この鍵をセッション鍵という)、これをカード鍵kで暗号化してICカード6へ送信する(ステップS7)。これと同時に音声信号をセッション鍵で暗号化し、端末1へ送る。暗号化された音声信号は端末1の大容量メモリ8に一旦格納される(ステップS8)。一方暗号化されたセッション鍵はICカード6の第1の復号手段9で復号され、元のセッション鍵に復元される。この復元されたセッション鍵を用いて第2の復号手段10により、大容量メモリ8に格納されている暗号化された音声信号は元の音声信号に復元され、曲の再生が可能となる。その後端末1のディスプレイ上の「スタート」という表示を指で押すと、演奏が開始される。

【0019】演奏が終わると、ディスプレイには例えば(1)鑑賞、(2)録音、(3)終了の選択枝が表示される。別の曲を聴きたい場合は(1)を選択し、ステップS6またはステップS4から同様の処理を繰り返す。また、今聴いた曲を録音したい場合は(2)を選択する。(2)が選択されると、その情報がセンター3へ送

5

られる（ステップS 9）。センター3が録音指示を端末1に送ると（ステップS 10）、大容量メモリ8から記録メディア7へ暗号化された音声信号が書き込まれる。これにより、ICカード6を所持する正当なユーザは、繰り返しその曲を聴くことができ、また、バックアップや編集のような個人利用のために暗号化された音声信号をデジタルコピーすることも可能である。しかし、記録メディア7の内容を別の記録メディアにコピーして複製を作ったとしても、書き込まれた音声信号は暗号化されているため、このユーザのICカード6がないと音声信号を復元し再生することはできない。このようにして、不正コピーを防止することができる。

【0020】本サービスを終了する場合は（3）を選択すると、決済処理へ移る（ステップS 11）。決済処理では、録音しなかった場合、聴いた回数分だけICカード6の口座から料金が差し引かれるが、これは比較的低額に設定される。一方、録音を行った場合は、録音料金が差し引かれるが、これは比較的高額に設定される。

【0021】次に各ステップを説明する。図3はステップS 3のカード認証の一例を示したものである。まず、ICカード6は会員番号格納部11に格納されている会員番号nをセンター3へ送信する。センター3はカード鍵演算部12において関数Fを用いて会員番号nからカード鍵kを算出する。カード鍵kは各ICカードに固有の秘密番号である。すなわち、カード鍵kは、このICカード6のみが有し、センター3のみが会員番号nから算出し得る秘密の番号であり、カード認証、コピー防止、決済というセキュリティに関する全ての処理に使用される極めて機密性の高いデータである。

【0022】次にセンター3は乱数生成手段13を用いて乱数rを生成し、ICカード6へ送信する。ICカード6は演算部14により、カード鍵格納部15に格納しているカード鍵kを用いて乱数rに演算Gを施し、センター3へ送信する。このデータをx 1とすると、x 1は次式で表される。

$$【0023】x 1 = G(k, r)$$

センター3は演算Gを行う演算部16を有しており、先に算出したカード鍵kで乱数発生手段13が生成した乱数rに演算Gを施し、x 2を算出する。比較手段17はx 1とx 2を比較し、これらが等しい場合、ICカード6がカード鍵kを有する正当なカードであるとみなし、カード認証のステップS 3を正常に終了する。x 1とx 2が異なっている場合は、不正なカードによるアクセスであるため、サービスは打ち切られる。

【0024】次に図4を用いてセッション鍵の配送（図2のステップS 7）および音声信号の送信（ステップS 8）を説明する。まず、センター3はセッション鍵生成手段18を用いてセッション鍵sをランダムに生成する。そして、暗号化手段19において演算Gを施し、前述のカード鍵kによりセッション鍵sを暗号化してIC

6

カード6に送信する。このデータをyとすると、yは次式で表される。

$$【0025】y = E(k, s)$$

ICカード6は暗号化手段19によってyをセッション鍵sに復元する第1の復号手段9を有しており、これを用いてカード鍵kによりyをセッション鍵sに復元する。

【0026】次にセンター3は暗号化手段21において関数Pを用いて音声信号mを上記セッション鍵sで暗号化し、端末1へ送信する。このデータをzとすると、zは次式で表される。

$$【0027】z = P(s, m)$$

このデータzは大容量メモリ8に一旦格納された後、第2の復号手段10において第1の復号手段9で復元されたセッション鍵sにより元の音声信号mに復元される。

【0028】また、同じく図4を用いて録音要求（図2のステップS 9）が出された場合の処理と再生方法について説明する。端末1の録音要求部22からの録音要求を受けてセンター3の録音指示部23により録音指示が出された場合、ドライバ24を介して暗号化されたデータyと暗号化されたデータzが記録メディア7に記録される。録音されたデータzを再生するとき、記録メディア7に記録された暗号化されたセッション鍵のデータyがICカード6に入力され、前述と同じ処理によりセッション鍵sが復元され、それを用いて暗号化されたデータzから元の音声信号mが復元される。

【0029】このようにカード鍵kを有するICカード6を用いれば音声信号mの復元が可能となるが、ICカード6がなければ、セッション鍵sを復元することができないため、音声信号mも復元することができない。

【0030】（実施例2）次にICカード6を所持するユーザが、ドライバ24を何らかの理由により操作し、センターが録音指示を出していないにもかかわらず記録メディア7への録音処理が行なわれた場合、このユーザはICカード6の所持者自身であるから音声信号の再生が可能である。すなわち、このユーザは録音のための料金を支払うことなく録音が可能となる。

【0031】この操作を防止する方法を図5を用いて説明する。図5は録音要求が出された場合の処理方法に関する他の実施例を示したものである。ステップS 7、S 8については同様であるため、説明を省略する。ステップS 9、S 10について説明するとICカード6が鍵処理部25とセッション鍵格納部26を有しており、ユーザからの録音要求があった場合（ステップS 9）、鍵処理部25は乱数uを生成し、出力する。録音要求部22はこの乱数uをセンター3へ送信する。録音指示部23は、この乱数uをカード鍵kで暗号化してデータvを生成し、vとともに録音指示を端末1に送信する（ステップS 10）。これにより、ドライバ24を介して暗号化された音声信号データzが記録メディア7に記録され

る。本実施例では、暗号化されたセッション鍵データ y は記録メディア 7 には記録されない。一方、信号データ v は IC カード 6 に与えられ、鍵処理部 25 により検証される。この検証結果が正しければ、セッション鍵 s' がセッション鍵格納部 26 に書き込まれる。再生の際には、この格納されたセッション鍵 s' が読み出され、音声信号 m の復号のために使われる。本実施例では、ユーザが前記のような操作を試みても、IC カード 6 は物理的に安全であるため、鍵処理部 25 を操作してセッション鍵 s' を不正に書き込むことはできない。また、録音指示部 23 からの信号データ v を偽造しようとしても、この信号データ v はカード鍵 k と乱数をもとに暗号化されているため、偽造は不可能である。このように、録音指示により音声信号 m を復号するためのセッション鍵 s' を IC カード 6 に書き込む方法を採用することにより、なお一層、セキュリティを向上させることができる。

【0032】ただし、再生の際に IC カード 6 から読み出されるセッション鍵 s' の盗聴に関しては注意を払わなければならない。なぜならば、盗聴されたセッション鍵 s' を記録した媒体と、暗号化された音声信号の複製との組み合わせにより、音声信号の再生が可能となるからである。

【0033】これを防ぐための一つの手段は、IC カード 6 からセッション鍵 s を読み出して音声信号全体を復号するのではなく、復号手段 10 と IC カード 6 とが連動して音声信号 m を復号することである。例えば、音声信号の復号の一部を IC カード 6 内で行うようにする。この復号処理を IC カード 6 に行わせるための IC カード 6 への命令は、制御情報として、暗号化された音声信号が m に付加して記録メディア 7 に記録される。このような処理を複雑にし、かつ秘密にすることにより、単なるセッション鍵 s' の盗聴で音声信号 m を再生することは不可能となり、セキュリティはより一層向上する。

【0034】最後に決済処理（図 2 のステップ S11）について図 6 を参照しながら説明する。センター 3 のトランザクションデータ送信部 27 は会員番号、日付、金額等の情報からなるトランザクションデータ t を IC カード 6 に送信する。ここで金額については既に述べたとおり、録音しなかった場合と、録音した場合では、差が設けてある。IC カード 6 の署名生成部 28 は、IC カード 6 内の口座の残高から支払額を減算した後、署名鍵格納部 29 に格納された署名鍵 c を用いて関数 H によりトランザクションデータ t に対する署名データ a を生成する。署名データ a は、 $a = H(c, t)$

で表され、センター 3 に送信される。センター 3 はメモリ 30 にトランザクションデータ t と署名データ a とを対にして記録する。

【0035】ここで署名鍵 c は IC カード 6 に固有であ

り、図 1 の銀行 4 のみを知る秘密鍵である。センター 3 も署名鍵 c を知らないので、署名データ a を偽造することはできない。したがって、署名データ a はトランザクションデータ t に対するユーザの署名とみなすことができる。これらのデータを図 1 の専用回線 7 を用いて銀行 2 に送信することにより、銀行 2 内で処理が行われ、決済が完了する。

【0036】これまで述べてきた通り、IC カードを用いた本実施例のシステムにより、ユーザは相応の料金を支払えば音楽ソフトをデジタル録音することが可能となる。その他、IC カードを用いることにより、本実施例は次の効果を奏する。

【0037】まず第 1 に、システムへのアクセスツールとして IC カードを用いているため、IC カードを所持し、かつ、その IC カードの暗証番号を知らなければシステムにアクセスできないため、暗証番号のみによるアクセスに比べセキュリティが高い。

【0038】第 2 に、決済処理が IC カードを用いて行われているため、ユーザは IC カードさえ所持しておれば、どの端末を用いても本サービスを受けることができるという点である。すなわち、ユーザはいろんな場所にいながらにして、このシステムを利用できることとなり、利便性が増す。

【0039】本実施例では、音楽ソフトの場合を例に上げて示したが、これに限定されることなく、本発明は映像ソフト、ゲーム等、デジタル化された情報に関するあらゆるサービスに適用し得るものである。

【0040】

【発明の効果】以上のように本発明によれば、IC カードに格納された秘密のカード鍵によってのみ、記録メディアに記録されたデジタル情報が復元可能となるため、この IC カードがなければ実質的なコピーは得られなく不法コピーを防止できる。また、センターからの録音指示により、デジタル情報を復元するための秘密情報を IC カード内に書き込む手段を設けることにより、正当な支払をすることなくデジタル録音するようなユーザの操作を防止することができる。さらに、IC カードのカード鍵を用いてカード認証を行うことにより、不正アクセスに対する防御を強固にできる。また、IC カードのカード鍵を用いて決済処理を行うことにより、端末ではなく IC カードによる決済が可能となり、ユーザは本システムを利用するための端末を限定されることなく利便性が高い。

【図面の簡単な説明】

【図 1】本発明の一実施例におけるシステムの概略を示す図

【図 2】本発明の一実施例の処理フローを示す図

【図 3】本発明の実施例のカード認証ステップのブロック図

【図 4】本発明の実施例のデジタル情報の送信および録

音ステップのブロック図

【図5】本発明の他の実施例のデジタル情報の送信および録音ステップのブロック図

【図6】本発明の実施例の決済ステップのブロック図

【符号の説明】

1 マルチメディア端末

2 ISDN

3 センター

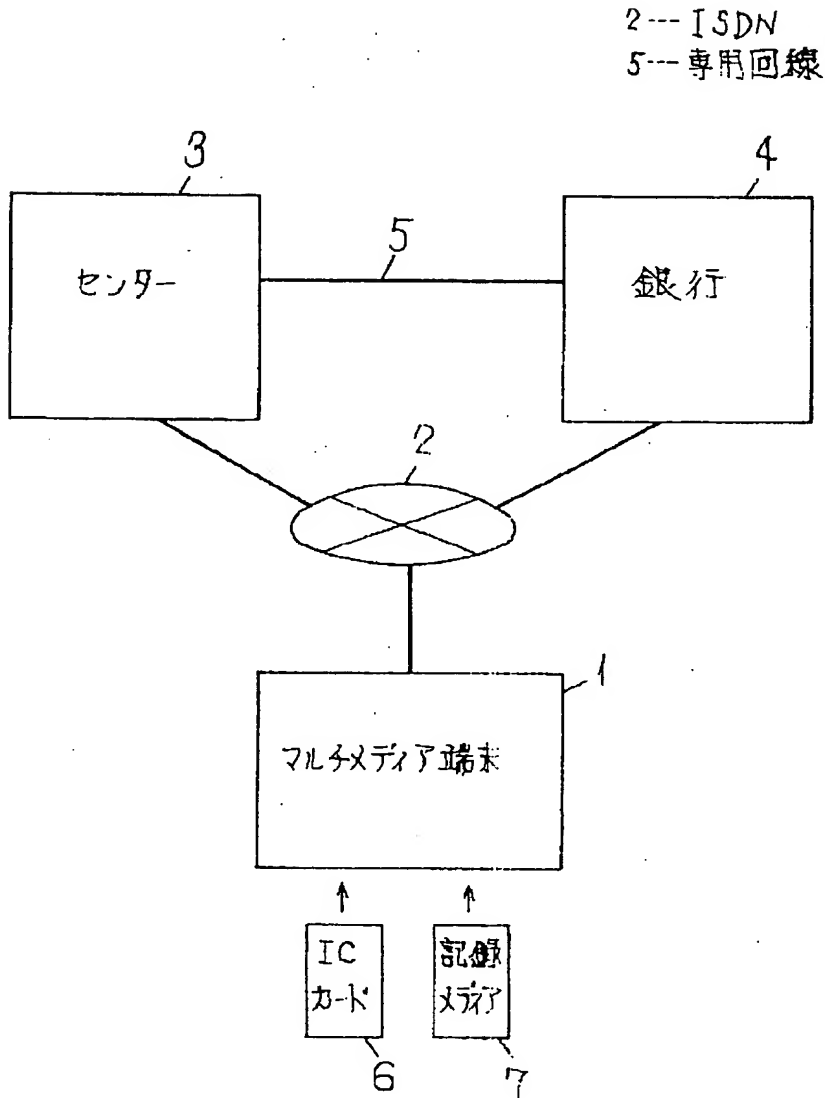
4 銀行

5 専用回線

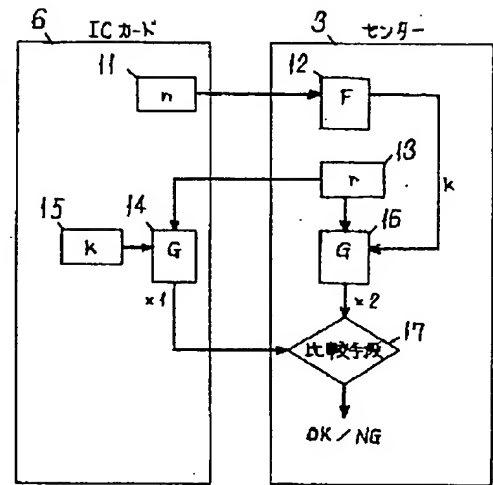
6 ICカード

7 記録メディア

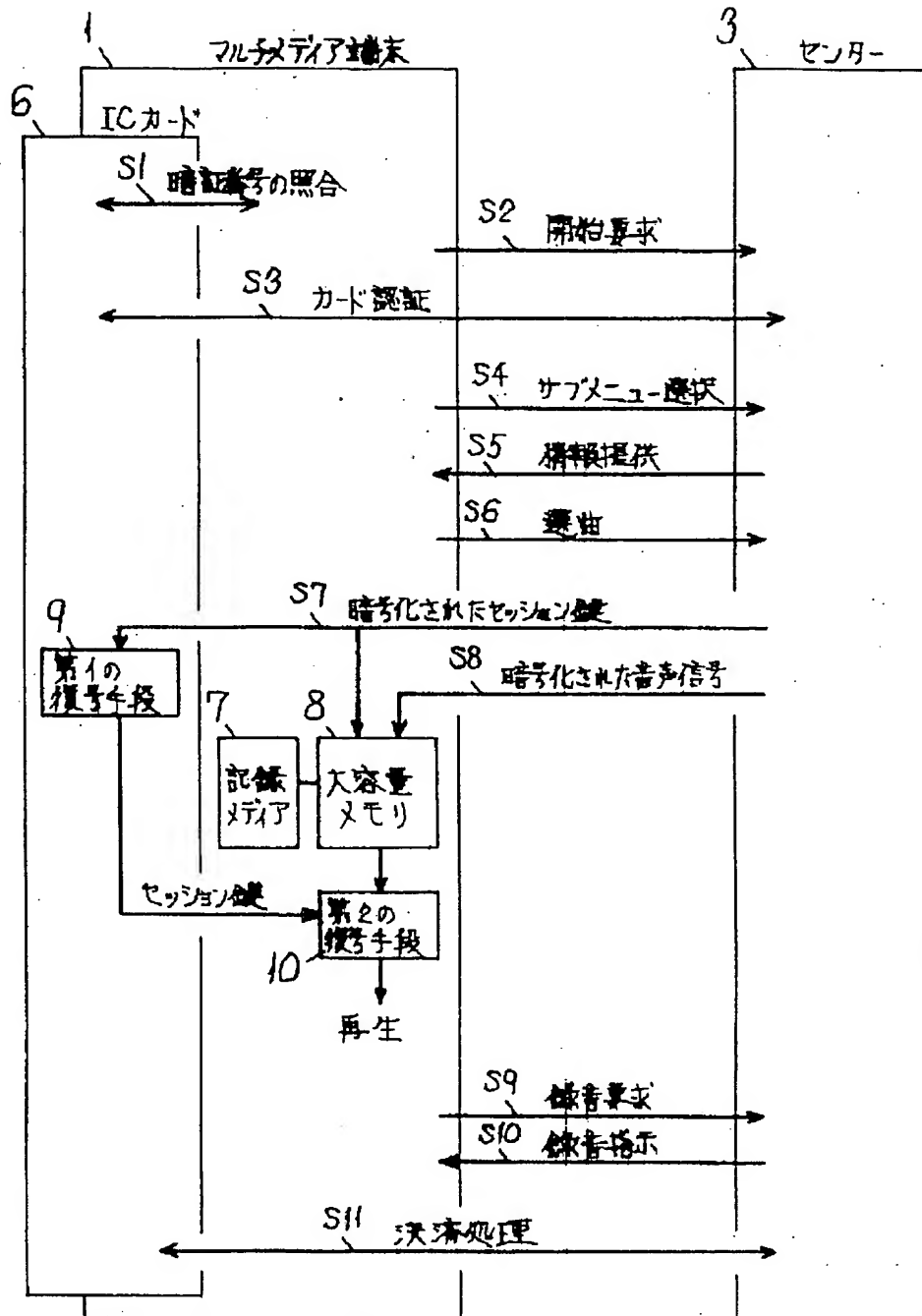
【図1】



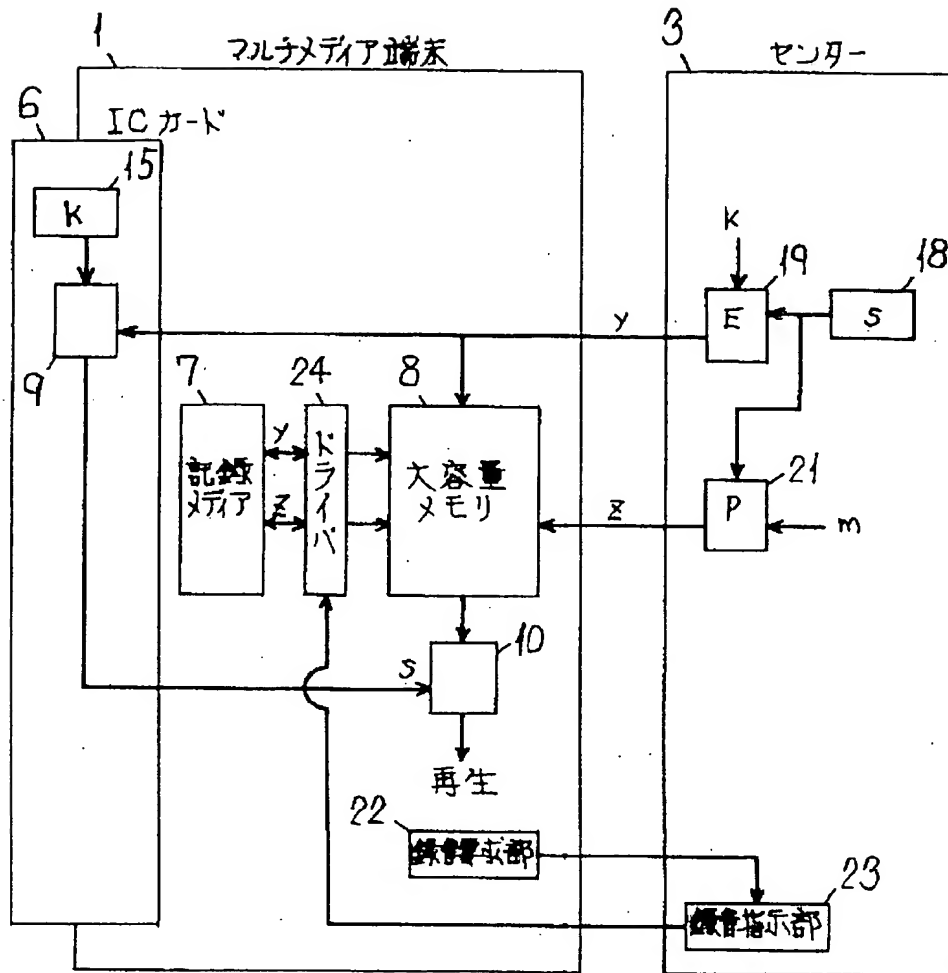
【図3】



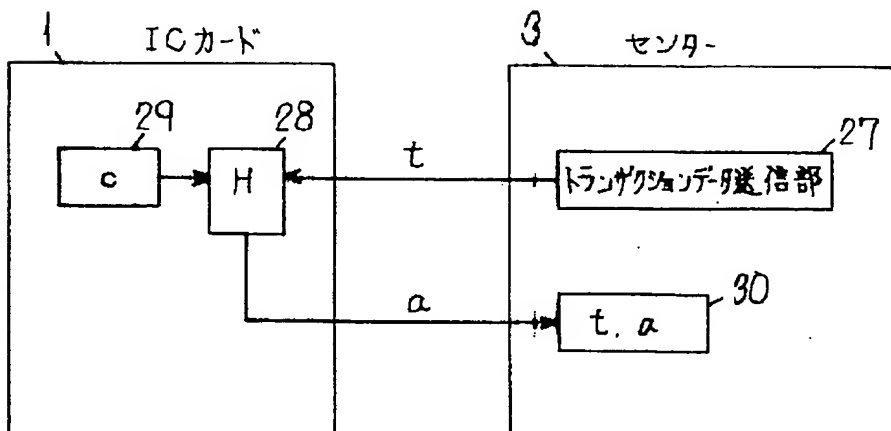
【図2】



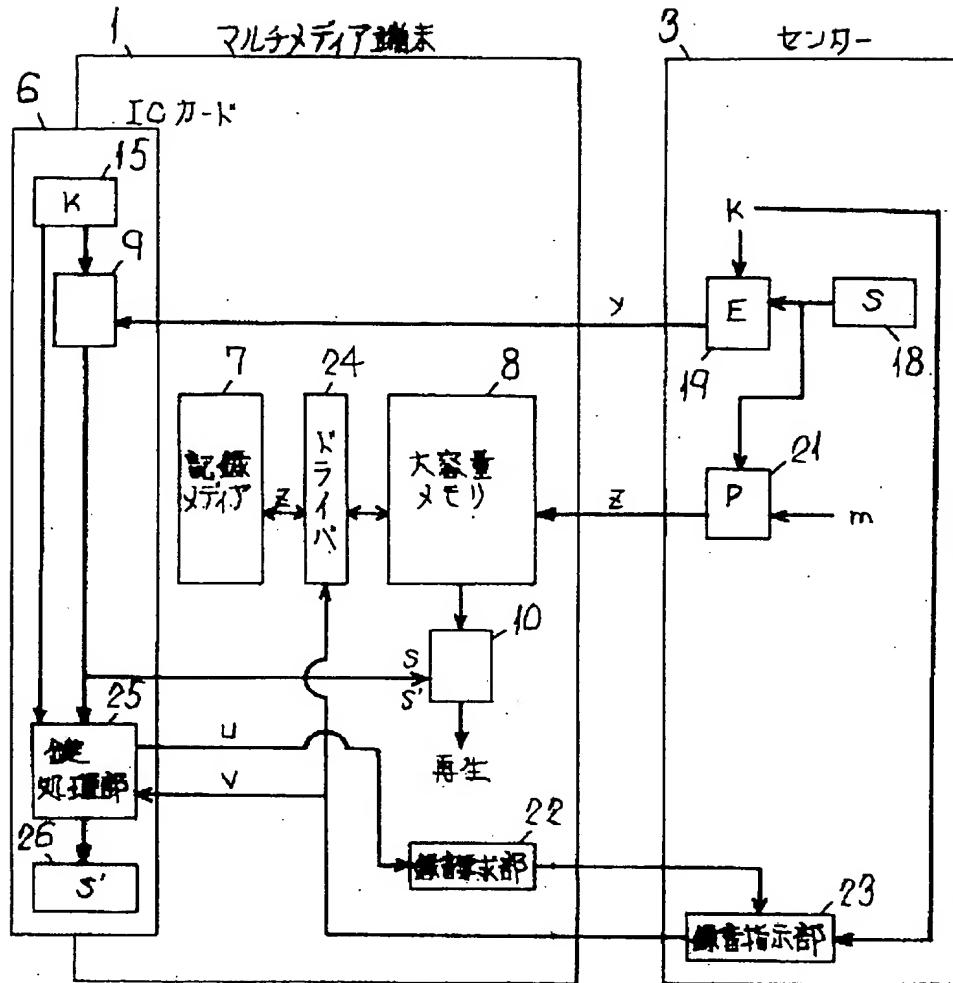
【図 4】



【図 6】



【図 5】



フロントページの続き

(51) Int. Cl. ⁶

識別記号

庁内整理番号

FI

技術表示箇所

H O 4 H 1/02

$$\mathcal{Z}$$

H O 4 L 9/00

9/10

9/12

H O 4 N 7/173

E